A Framework for Managing Faults and Attacks in WDM Optical Networks

Jigesh K. Patel, Sung U. Kim, David H. Su
National Institute of Standards and Technology
Gaithersburg, MD 20899
{Patel,kimsu,dsu}@antd.nist.gov

Suresh Subramaniam, Hyeong-Ah Choi
The George Washington University
Washington, DC 20052
{suresh,choi}@seas.gwu.edu

Abstract

Fault and attack survivability issues concerning physical fiber security in all-optical transport networks (AOTNs) require a new approach taking into consideration AOTN physical characteristics. Furthermore, unlike in electronic networks that regenerate signals at every node, attack detection and isolation schemes may not have access to the overhead bits used to transport supervisory information between regenerators or switching sites to perform their functions. This paper presents an analysis of attack and protection problems in AOTNs and proposes a conceptual framework for modeling attack problems and protection schemes for AOTNs.

1. Introduction

Core transport networks are currently in a transition period evolving from SONET/SDH-based Time Division Multiplexed (TDM) networks utilizing a single wavelength to the Wavelength Division Multiplexed (WDM) networks with multiple wavelengths strictly for fiber capacity expansion, and most recently, toward WDM-based all-optical networks. In all-optical networks, the transport, multiplexing, routing, supervision, and management of network survivability are all done at the optical layers. In all-optical transport networks (AOTNs), short and sporadic failures of network elements (e.g., fiber link, optical cross-connect (OXC), optical add-drop multiplexer (OADM), etc.) may cause a large amount of data loss. The widespread deployment of high-capacity WDM systems in the core transport network continues, and the survivability of WDM AOTNs in the presence of faults and attacks is becoming a critical issue and currently receives great attention from the research community.

The maturity of optical network elements such as OXCs and OADMs, and of terminal and line devices such as lasers and amplifiers has enabled the optical network designer to rapidly provision *lightpaths* and switch them via *wavelength routing*. A lightpath is an all-optical path over which data is carried on a single wavelength. The wavelengths are capable of being dynamically switched inside the optical network by OXCs that are not sensitive to the signal itself, but only to the wavelength over which it is carried. Such routing is called wavelength routing and renders the lightpaths transparent to variables such as modulation format, bit-rate and protocol type. Nevertheless, several impairments diminish the signal quality and the signal may have to be regenerated at certain points in the network. We therefore model the core network infrastructure to consist of all-optical sub-networks (islands) that are connected together using the regenerators (Figure 1). In this paper, we focus only on fault and attack management of an all-optical network, and hence assume that network monitoring schemes that imply opto-electronic conversion are unavailable. We propose a conceptual framework for the management of faults and attacks in an AOTN that is based on a previously proposed architectural model.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2001		**00-00-2001 to 00-00-2001**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A Framework for Managing Faults and Attacks in WDM Optical Networks	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Institute of Standards and Technology,Gaithersburg,MD,20899**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Proceedings of DARPA Information Survivability Conference and Exposition (DISCEX 2001), June 12-14, 2001, vol. II, pp. 137-145

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**12**	

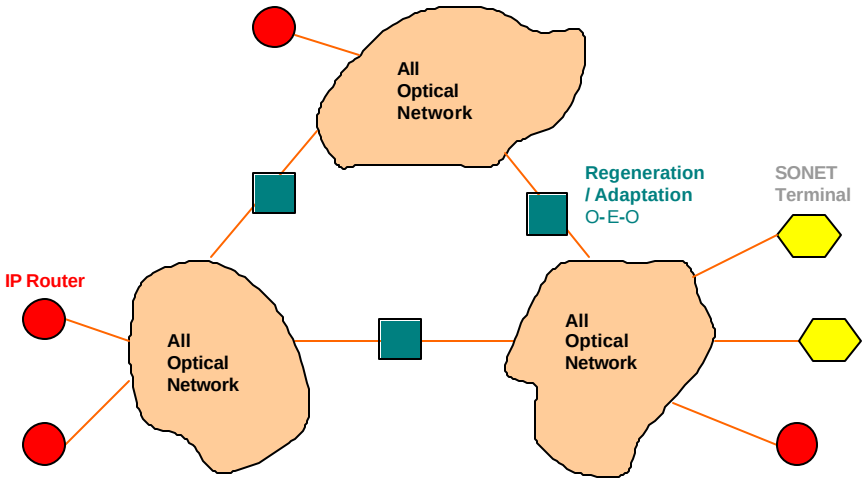
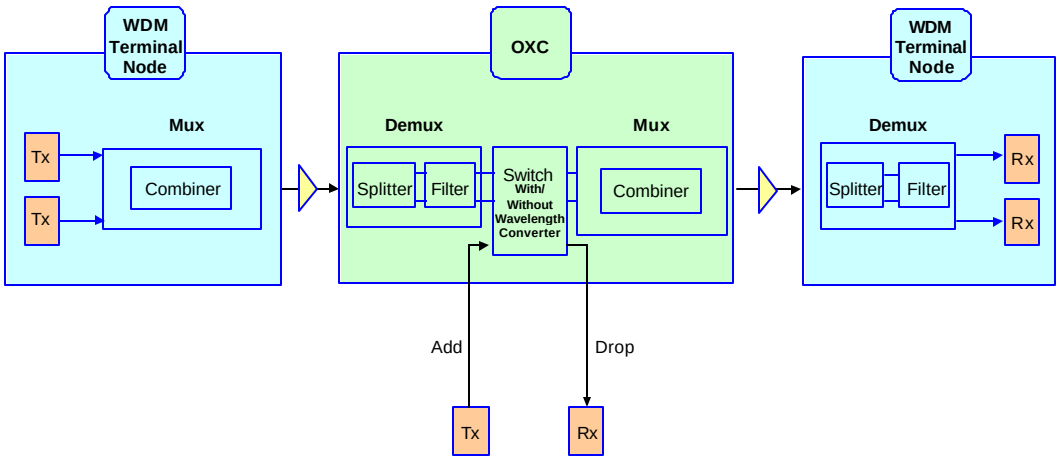


Figure 1. Networking infrastructure with all-optical sub-networks connected by regenerators.

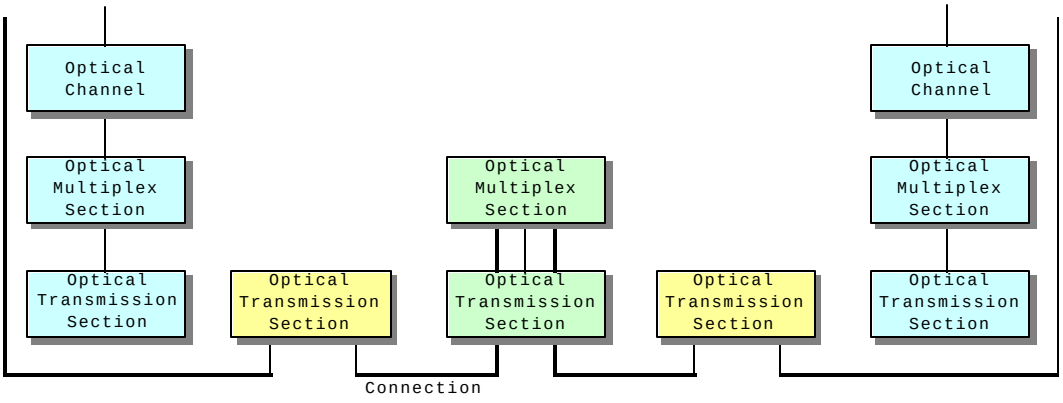
Four key research issues can be identified for fault and attack management in WDM optical networks, namely, fault and attack modeling, detection, localization, and protection/restoration. Each of these issues will be discussed in the paper. The rest of the paper is organized as follows. The architecture of an AOTN is presented in Section 2. A framework for fault and attack management is outlined in Section 3. We also discuss possible faults and attacks on the optical layers, detection and localization, and protection/restoration issues. Finally, our conclusions are presented in Section 4.

2. AOTN Architecture

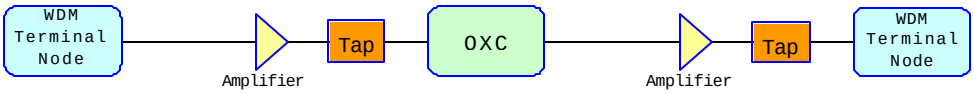
An AOTN is a network where the user-network interface is optical and data does not undergo optical to electrical conversion within the network. AOTNs using WDM transmission techniques and employing Micro-Electro-Mechanical System (MEMS) technology, will be commercialized with capacities greater than 1 Tb/s over a single fiber in the near future. One of the distinguishing characteristics of AOTNs is the fact that AOTNs are typically used to carry extremely high data rates. Consequently even faults or attacks that are short and sporadic can result in large amounts of data being corrupted or compromised. AOTN introduces new physical components such as optical add/drop multiplexers (OADM) and optical cross connect/wavelength routing switches (OXC/WRS) that may change potential modes of attack from those that are known for electronic or electro-optic networks. Figure 3 represents a model of AOTN. Note that the upper part of Figure 3 shows a configuration of the AOTN and the lower part, a corresponding layered architecture for AOTN as described in ITU-T G.872 [10]. A lightpath consists of a number of intermediate OXCs between the source and the destination nodes (which may be OXCs or WDM line terminals), interconnected by fiber segments, amplifiers and optional taps. The optical components that constitute an OXC include a switch (with or without wavelength conversion functionality), a demultiplexer comprising signal splitters and optical filters, and a multiplexer made up of optical filters and signal combiners. An OXC may also contain a transmitter array (Tx) and a receiver array (Rx) enabling local add/drop of the wavelengths.



(a)



(b)



(c)

Figure 2. A model of AOTN

The functionality of an AOTN can be decomposed into the following hierarchical layers (from top to bottom) [10]: Optical Channel (OCh) layer, Optical Multiplex Section (OMS) layer and Optical Transmission Section (OTS) layer. The OTS layer provides optical signal propagation functionality and represents the transmission medium, taps and amplification modules. The OMS layer enables wavelength routing functions, and the OCh layer handles channels for information content. In the next section, we discuss faults and attacks in AOTNs and present our framework for their management.

3. A Framework for Fault and Attack Management

3.1. Faults and Attacks

An optical signal undergoes many transmission impairments throughout its route. These impairments range from simple attenuation to complex nonlinear effects and polarization dependent losses. The peculiar behavior of the fiber transmission medium and active/passive elements in the network makes an AOTN vulnerable to unscrupulous attacks, thereby jeopardizing the security of information. These attacks may range from a simple physical access to the medium and its subsequent manipulation, to more complex exploitations of characteristics of optical devices on the link. The attacks related to the physical access of medium or devices are easier to detect and rectify. On the other hand, attacks exploiting device characteristics necessitate more involved diagnostic expertise, complex remedial measures, even more systematic detection schemes and control protocols.

Relative to electronic networks, optical networks require additional attention in terms of fault and attack modeling for several reasons. First, optical components and architectures have substantially different accessibility and vulnerabilities from electronic components. For instance, it is fairly straightforward to tap or jam signals at a specific wavelength by bending an optical fiber slightly and either radiating light out of it or coupling light into it [20]. Second, the physical properties of transmission create unique opportunities for the determined attacker. The particular physical property of interest is the transparency of lightpaths. This refers to the fact that, unlike electronic counterparts, optical components along a connection do not process the user payload. Unfortunately, this transparency allows an intruder that has gained access to one component to simply pass a signal right through all the components that handle the associated lightpath. This means that a signal can be forced into the network at a remote location and, by judicious choice of wavelength, affect many different parts of the network. Such a widespread effect is hard to achieve in conventional networks because signals are regenerated at every node, and therefore, a malicious physical signal can be trapped at the ends of a link. Third, optical technology allows for different attack opportunities; for example, the crosstalk level in switches may be sufficiently low for normal operation but may not be low enough to prevent an attacker from transmitting a high-power jamming signal that would disrupt service.

The management of attacks involves the protection of secure data. The security can be at the logical (or semantic level) (i.e., protect the meaning of the data if an attacker is able to obtain them) or at the physical level (i.e., protect the data from being accessed/disrupted by the attacker) [20]. This paper is restricted to the physical security aspect. In general, fault and attack survivability in AOTNs can be summarized as illustrated in Figure 4.

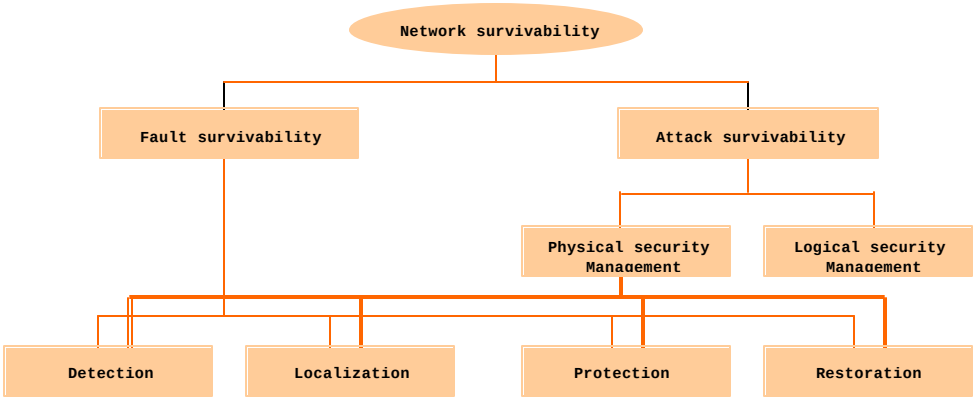


Figure 3. Network survivability.

The main goals of fault survivability (fault management) are to set up routes in anticipation of faults (protection), locate the faults (detection and localization), and to re-route the affected connections (restoration). Protection is the primary mechanism used to deal with faults. In protection, preplanned

protection resources (fibers, nodes, etc.) are set aside for restoring traffic when the working path is established. On the other hand, restoration dynamically discovers an alternate route from spare resources in the network for disrupted traffic, once a fault is detected. Fault detection is one of the crucial functions and a prerequisite for the above mentioned protection/restoration schemes. The inability of AOTNs to reconstruct data streams at nodes and amplifiers within transparent networks complicates segment-by-segment monitoring of communication links. Nevertheless, many common faults (such as fiber cuts and node malfunctions) may be detected by optical monitoring methods. On the other hand, a resourceful attacker may thwart detection with the relatively simple monitoring methods available now. Although research on attack survivability for AOTN is relatively scant, many interesting issues exist [20]. The following is a brief review of the literature in this area that we are aware of.

Ramaswamy and Humblet [7] have analyzed amplifier induced crosstalk and saturation components that may be potentially used by an intruder for service disruption. Medard, Chinn, et al. [4] have considered the case when an erbium doped fiber amplifier (EDFA) is under attack. The detection technique in [4] involves both optical and electronic signal processing, and is commercially non-feasible at this time. Zhou, et al. [8] and Gillner, et al. [9] provide extensive analysis of cross-talks on AOTNs. While unintentional crosstalk may result in an unauthorized access to critical information, it can also intentionally lead to disruption of service at the behest of a malicious attacker.

Note that many of the traditional security problems related to logical security present in traditional electronic networks are still present in AOTNs. However, a new approach for logical security (i.e., encryption, privacy and authentication) taking into consideration AOTN physical characteristics may be investigated.

3.2. Conceptual Modeling of Attacks

Figure 4 shows a typical AOTN link with ports vulnerable to possible attacks numbered. We present here a brief description of transmission impairments and possible types of attacks each of these ports may experience.

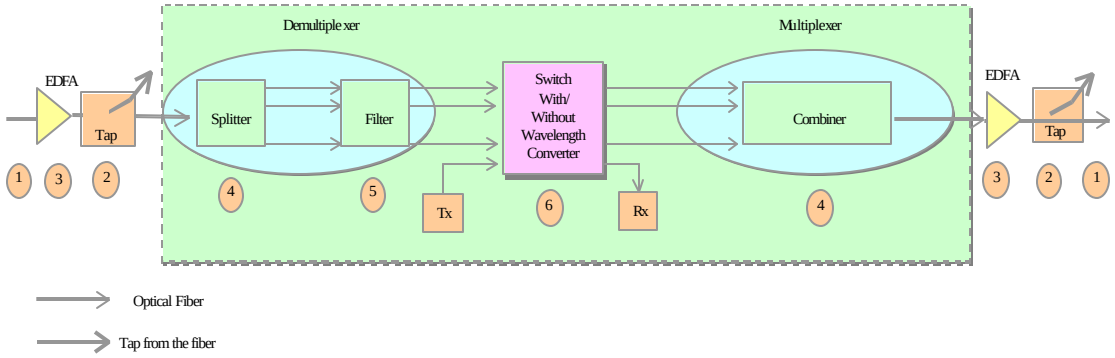


Figure 4. An Optical Cross-Connect (OXC) node.

3.2.1. Fiber (attack point 1 in Figure 4). An optical signal carrying high-speed data will experience attenuation, dispersion, non-linear effects and polarization dependent losses. While the use of amplifiers can solve attenuation, amplifiers also contribute additional impairments. The use of specific types of fibers (such as dispersion-shifted, polarization-maintaining fibers) may be suggested for reducing dispersion and polarization related degradations, but they, in turn, may introduce other problems such as crosstalk. The unprotected easy access to the physical fiber cable can encourage tampering with by a potential intruder. Simple physical attacks like cutting of the cable can easily be detected by existing metrology techniques and can also be prevented by increasing physical security-related measures. On the other hand, easy physical access to the fiber cable can also cause unauthorized access and subsequent manipulation of the information by way of tapping or by sensing the optical mode leakage. In order to

detect this kind of information, more sophisticated measurement techniques are needed.

3.2.2. Tap (attack point 2). The purpose of providing taps is to facilitate easy monitoring, and providing efficient splicing ports for increased demand thereby adding flexibility to the network. Insertion loss and information leakage are associated transmission impairments which can again be eliminated by using amplifiers at the expense of additional vulnerability to attacks as we shall see next. Access to taps also provides an opportunity to the attacker to have access to the signal and to tamper with it by way of either changing the signal power or signal polarization or similar signal properties. This can create problems for subsequent amplifiers and other polarization sensitive network elements and may result in service disruption. Such tampering can be thwarted by minimizing the number of taps and by increasing the physical security in order to prevent access, but detection of a tampered signal may not be easy.

3.2.3. Erbium Doped Fiber Amplifiers (attack point 3). Semiconductor optical amplifiers (SOA) have bandwidths of the order of 100 nm, which is much higher than those of EDFAs (35nm). On the other hand, it is possible to have high gains and output powers with EDFAs. Also, SOAs introduce severe crosstalk when used in WDM systems [11] and so EDFAs are widely preferred and used for AOTN. In addition to amplified spontaneous emissions (ASE) and necessity for flattening the gain spectrum, EDFAs introduce a system penalty in the presence of other interfering channels. This system penalty can be decomposed into two components. The first component arises from the *steady-state* reduction in the amplifier gain due to the increase in the *average* input power. This is also referred to as the *saturation component*. The second component is the component arising from the variation in the gain due to the randomness of the total input power around the mean value. This is known as the *crosstalk component* [12]. It is known that when the number of channels is small, the cross-talk component dominates, but when the number of channels is large, the saturation component dominates. For high data-rate transmission (i.e., data rates much higher than the response time of the amplifier to a change in input power level), the cross-talk component is no longer present and only the steady-state gain reduction is retained [7]. An intruder can easily block transmission of other channels or can disrupt the entire service merely by exploiting this weakness of the EDFAs. Even a legitimate user can cause an attack by transmitting at high power levels so as to deteriorate EDFA performance. The use of multi-stage EDFAs in a link requires extra precautions and system margins**.** One can detect this kind of attack by *in situ* verification of the following equality around the EDFA if along the link or around the cross-connect or node (if it employs EDFAs as an integral part): $\lambda_i = \lambda_o \pm \lambda_{d/a}$ where λ_i is total number of wavelength at the input of the "block" (can be an EDFA or an OXC node), λ_o is the total number of wavelengths at its output and $\lambda_{d/a}$ is the total number of wavelengths dropped or added at the node by OADMs. One possible solution we propose to mitigate this type of attack is to equalize gain by way of pre-emphasis and de-emphasis as the case may be, before sending the signals to the EDFA. This can be done by optical processing or by electronic processing with their obvious inherent merits/demerits.

3.2.4. Splitter/Combiner (attack point 4). Typically, a demultiplexer comprises of an optical splitter followed by an optical filter. The power loss introduced by a splitter is its insertion loss. If the splitter itself also performs the function of a filter, it can cause signal degradation and can pose vulnerability to intentional attacks as described below for the case of a filter.

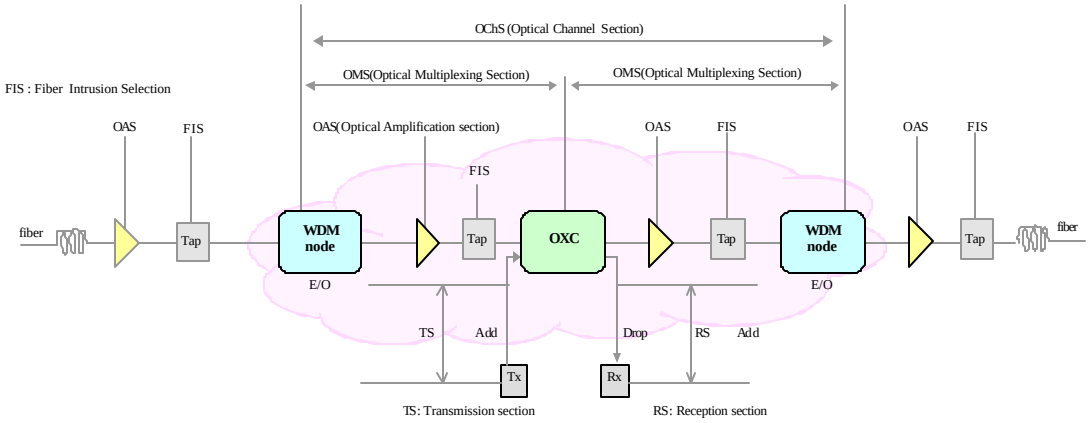
3-2-5. Filter (attack point 5). A good optical filter should have a low insertion loss. The loss should also be independent of the state of polarization of the input signals. The filter should be insensitive to variations in ambient temperature. As more and more filters are cascaded in a WDM system, the passband becomes progressively narrower. To ensure reasonably broad passbands at the end of the cascade, the individual filters should have very flat passbands. At the same time, the passband skirts should be sharp to reduce the amount of energy passed through from the adjacent channels. This energy is seen as crosstalk and degrades the system performance. This crosstalk can also result in an unauthorized access to information. An intentional high power level may subsequently result in high crosstalk levels thereby blocking other legitimate users and can constitute an intrusion. This type of attack is not easy to detect and not easy to rectify on-line. Precautionary measures include power equalization before and after filtering and the use of high quality optical filters.

3.2.6. Switch (attack point 6). An optical switch also is subject to crosstalk due to non-ideal switching. When an interfering signal has been suppressed once with reference to the main signal, it results in a first-order crosstalk. If it is suppressed twice, it results in a second order crosstalk, and so on. Due to multiple

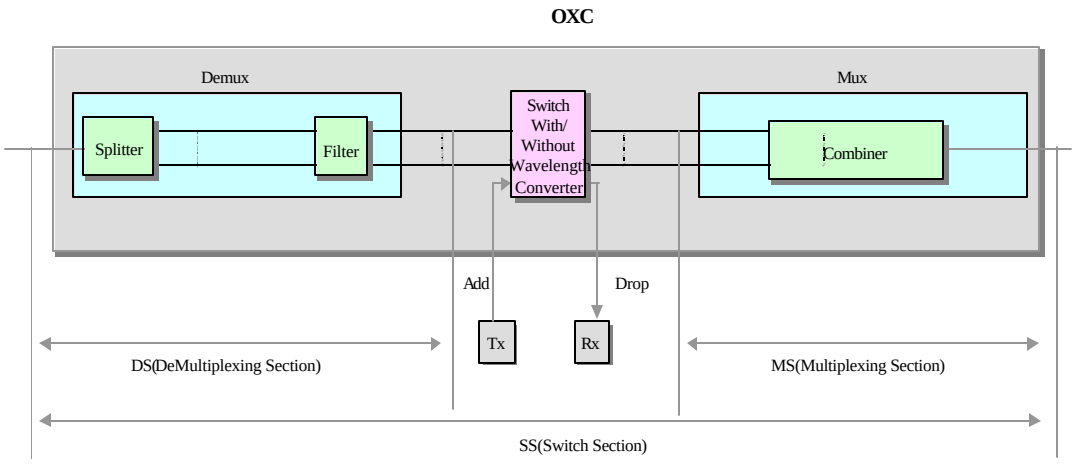
switches and multiple nodes in a network, propagation of crosstalk becomes more and more complex. An intruder can also exploit polarization dependent properties of switches and filters to cause service disruption by way of manipulating the signal polarization. A legitimate user can also cause serious threats by changing transmitter power levels and thereby introducing intentional crosstalk to disrupt service or can utilize sensitive reception techniques to gain unauthorized access to the information from crosstalk. While equalizing power levels will eliminate the former type of attack, the latter type of unauthorized information access is not easy to detect. Non-blocking type of switches may also employ wavelength converters and thereby can also contribute to crosstalk in addition to the associated noise, insertion loss and polarization dependent losses.

3.3. Analysis of Attack Management

In this subsection, we describe attack management using the management section model illustrated in Figure 5. The upper part of Figure 5 shows management sections for AOTN element attacks and the lower part, for an OXC node. With reference to the model as shown in Figure 5, we can categorize the issue of attack management at the following three functional levels:



(a)



(b)

Figure 5. Management sections.

3.3.1. Management of Direct Attacks. As we mentioned in section 3-1, there are certain physical link elements with their own peculiar characteristics that are more likely to be exploited by an intruder as direct attack ports. This creates a need for comprehensive management tools at physical and upper layers. Table 1 summarizes sub-sections that fall under this category along with corresponding attack detection, isolation and restoration features.

Subsections	Characteristic Attack	Detection and Isolation Mechanism	Recovery Mechanism
TIS	1. Tapping only	Continuous monitoring of average power levels before and after the tap	Bypass
	2. Tapping and jamming following signal processing	Difficult to decide whether anomaly or attack	
	3. Jamming only	Difficult	
OAS	1.Gain competition due to local attack	In-situ channel equality test (Section 3.2.3). Difficult.	Switch to protection bank of amplifiers
	2. Gain competition due to remote attack		
	3. Crosstalk	Difficult to detect as attack without electronic conversion (and subsequent BER measurements)	Equalize input power levels
OTS	Fiber cut	Standard fault localizing metrology	Switch to protection OChS/OMS

Table 1: Direct attacks and management functions

3.3.2. Management of Indirect Attacks. There are certain sections that are unlikely to be attacked directly either because a direct attack is too complicated to generate the desired effect or because the ports are not easily accessible to the potential intruders. Although these are less likely attacks, their detection, isolation and restoration become too complex, costly and debatable. Table 2 summarizes management-related issues for such attacks.

Subsections	Characteristic Attack	Detection and Isolation Mechanism	Recovery Mechanism
DS	Intentional crosstalk	Complex	Too costly - bypass traffic to backup DS
SS	1. Intentional crosstalk		Too costly - bypass traffic to backup SS
	2. Unauthorized access through add/drop ports		Difficult
MS	Intentional crosstalk propagation from preceding blocks		Too costly - bypass traffic to back up multiplexers

Table 2: Indirect attacks and management functions.

3.3.3. Management of Pseudo-Attacks. In dynamically reconfigurable networks, the quality of the signals may change significantly depending on the design of the physical network. For example, the add/drop of an extra wavelength at an OADM may influence the quality of the signals on other wavelengths.

These anomalies are not intrusions, but may be detected as attacks by intrusion surveillance algorithms. We call them as pseudo-attacks and these can be overcome in part or full by proper design implementation.

3.3. Detection and Localization

The detection of faults and attacks could potentially be faster at the optical layer than at higher layers. However, monitoring signals at the optical layers is usually limited to power and signal spectra measurements. No robust standard or technique exists to date for monitoring the network performance or for detecting faults and attacks at the optical layers. Recently, several schemes have been proposed for monitoring transparent optical channels (i.e., lightpaths): (1) monitoring optical channel continuity [1] through laser bias currents or the optically received or transmitted power levels, and (2) monitoring optical channel quality [2] through error-detecting codes, sampling methods, spectral methods, and indirect methods. Among these schemes, error-detecting codes are the best for estimating the bit error rates (BERs), but they require access to the electrical signals. Sampling methods are the most accurate for monitoring signals at the optical level. However, they are too difficult and complicated to be used in every network element. The spectral time averaging methods are simpler but ignore all distortion aspects, and are thus very inaccurate. Although standards based on these schemes are likely to emerge in the future, there has been some research on adapting schemes for electronic networks. For instance, attack detection and management schemes for amplifiers and fibers have been proposed in [3] and [4].

Fault/attack localization refers to the identification of the faulty component or source of attack. Very little is understood about this topic in AOTNs at this time. It is expected that sophisticated distributed algorithms would be required to accurately and precisely identify the location of faults. Attack

localization is even more challenging because attacks may propagate and affect several lightpaths over a wide geographical area.

3.4. Protection and Restoration

3.4.1. Optical Layer Level. Protection at the optical layers can be provided either at the OCh level or the OMS level in WDM ring networks. In the OCh protection approach, a failed lightpath can be fixed by converting an optical signal from a given wavelength into a different one, avoiding the rerouting of the signal. This is equivalent to span routing in SONET, with the difference that even two fiber WDM rings can provide such capability for OCh protection. Note that recent contributions to the ANSI T1X1.5 committee emphasize the need for automation of the OCh layer to establish optical channels in real time and provide a variety of protection levels depending upon user demand, ranging from 1+1, 1:1, to 1:N [13]. In the OMS layer, however, span protection will require four fiber rings, as in SONET. These extra features will undoubtedly introduce extra complexity in the optical layer automatic protection switching (APS) protocols. Because of the multiplicity of alternate routes, efficient protection in mesh networks is more complex.

To date, large-scale efforts are underway to develop standards that will run the fault (related to some kind of attacks) recovery function at WDM optical layers [2]. Within the optical layers, survivability mechanisms will continue to offer the fastest possible recovery from fiber cuts and flexible management of protection capacity. However, optical protection/restoration schemes are still in their infancy and it will take some time for standards to emerge. Overall, it is expected that WDM network survivability schemes will mirror SONET survivability schemes, implying both protection and restoration [14].

3.4.2. Electrical Level. One of the problems with pure optical transparency is that electronic frame-monitoring schemes cannot be applied in the AOTN's core to detect/localize faults and some kinds of attacks. Optical monitoring schemes for transparent optical channels are currently under investigation and standards are expected to emerge in the near future. Meanwhile, the frame-monitoring layer (i.e., optical adaptation layer) between WDM optical layer and the higher layer (e.g., IP layer) can be used for fault and attack detection and localization. However, per-channel monitoring inside the AOTN core will likely require some processing overhead such as O-E conversion and frame monitoring taking into consideration the signaling concepts (i.e., in-band or out-of-band signaling mechanism). In OIF and ANSI T1X1.5, the proposals for implementing frame-monitoring layer overhead information include the use of a TDM frame-like "SONET-lite" [15] or "digital wrapper" [16] to support OCh layer management functions such as performance monitoring, connectivity, and fault/attack indicator monitoring.

3.4.3. Control Protocol Level. Each of the IP/MPLS layer, adaptation layer, and the optical layer incorporates its own protection and restoration functions. Basically, the IP/MPLS over WDM framework provides three schemes according to protection/restoration granularity: fiber protection/restoration at the OMS level, channel protection/restoration at the OCh layer, and flow protection at the IP/MPLS layer. IP layer protection scheme uses traffic rerouting when failure or attack occurs inside the working entity. Within the MPLS framework, IETF draft [17] considered LSP restoration schemes. In this approach, in order to improve susceptibility to node and link faults (related to attack problems), hop disjointed backup routes can be used [18]. Although MPLS promises IP-layer protection with fast restoration and path switching, the Internet draft [19] comments that fast recovery is still hampered by Label Switched Path (LSP) failure detection. For example, even a single fiber cut or node failure will affect multiple LSPs, which means that hundreds of ingress routers of LSPs should be notified. Multiple LSP failures also lead to even more Label Switch Routers (LSRs) to update the topological and forwarding information. Within the MPLS framework, fiber-level protection schemes can be employed to improve this kind of scalability problem by using link-based LSP restoration concept in conjunction with the MPLS label stacking function. Nevertheless, this solution requires additional fiber diversity provision and fiber cut/switchover event. On the other hand, network service survivability within IP/MPLS over WDM requires that the survivability at optical layers very carefully could coordinate with the functions already provided by existing network layer protocols (ATM, SONET/SDH, etc.). In sum, in order to achieve maximum network survivability in optical MPLS networks, the implementation of protection/restoration, fault and attack detection and localization must be coordinated at both IP/MPLS layer and WDM optical layer.

4. Conclusions

An optical signal undergoes many transmission impairments throughout its entire path in an AOTN. The peculiar behavior of the transmission medium and active/passive elements in the network makes an AOTN vulnerable to unscrupulous attacks thereby jeopardizing the security of information. In AOTNs, data travel optically from source to destination without any optical-electrical conversions, thereby making the networks transparent to modulation format, bit-rate, and protocol. This transparency poses many survivability vulnerabilities to attacks. In this paper, we discussed in detail the possible attack scenarios at the physical layer and also presented a conceptual modeling of attack problems and possible protection schemes in AOTNs. However, attacks exploiting device characteristics necessitate comparatively more involved diagnostic expertise, complex remedial measures, even more systematic detection schemes and control protocols. Our future research will deal with the issue of practically feasible attack detection and restoration approaches.

Acknowledgement

This work was supported in part by the DARPA under grant N66001-00-18949.

References

[1] *Nelson L. E., Cundiff S.T., and Giles C.R.,*"Optical Monitoring using Data Correlation for WDM Systems", *IEEE Photonics Technology Letters*, Vol. 10, No. 7, Jul. 1998, pp.1030-1032.

[2] *C. P. Larsen, P. O. Andersson*, "Signal Quality Monitoring in Optical Networks," Optical Networks Magazine, Vol. 1, No. 4, Oct. 2000, pp. 17-23.

[3] *Li Chung-Sheng, Ramaswami R*, "Automatic Fault Detection, Isolation, and Recovery in Transparent All-Optical Networks," *IEEE Journal of Lightwave Technology*, vol. 15, no. 10, Oct. 1997, pp. 1784-1793.

[4] *Medard M., Chinn R., Saengudomlert, "*Attack Detection in All-Optical Networks," *Technical Digest of Optical Fiber Conference (OFC)*, 1998, pp. 272-273.

[5] *Hazan, J.P.; Steers, M.; Delmas, G.; Nagel, J.L.* ,"Buried Optical Fibre Pressure Sensor for Intrusion Detection," *Proceedings of 1989 International Carnahan Conference on Security Technology*,1989, pp. 149 - 154

[6] *Griffiths, B.*, "Developments in and Applications of Fibre Optic Intrusion Detection Sensors", Proceedings of 29th Annual 1995 International Carnahan Conference on Security Technology, Institute of Electrical and Electronics Security Technology, 1995, pp. 325 -330

[7] *Ramaswami R., Humblet P. A.*, "Amplifier Induced Crosstalk in Multichannel Optical Networks", *IEEE Journal of Lightwave Technology*, vol. 8, no. 12, Dec. 1990, pp. 1882-1896.

[8] *Zhou J., Cadeddu R., Casaccia E., Cavazzoni C., and O'Mahony, M. J.," Crosstalk* in Multiwavelength Optical Cross-Connect Networks", *IEEE Journal of LightwaveTechnology*, vol. 14, no. 6, June 1996, pp. 1423-1435.

[9] *Gillner L., Larsen C. P., and Gustavsson, M.," Scalability* of Optical Multiwavelength Networks: Crosstalk Analysis", *IEEE Journal of Lightwave Technology*, vol. 17, no. 1, Jan. 1999, pp. 58- 67.

[10] *ITU-T Rec. G.872*, "Optical Transport Networks", Feb. 1999

[11] *Ramaswami R., Sivarajan K. N.*, Optical Networks: A Practical Perspective, Morgan Kaufmann Publishers, Inc., CA, 1998.

[12] *Desurvire E.*, Erbium-Doped Fiber Amplifiers: Principles and Applications, John Wiley & Sons, Inc., NY, 1994.

[13] *Ghani, N. , Dixit S.*, "Channel Provisioning for Higher-Layer Protocols in WDM Networks", *Proceedings of the SPIE All Optical Networking Conference: Architecture, Control, and Management Issues*, Boston, MA, September 1999.

[14*] Manchester, J., Bonenfant, P., and Nowton, C.*, "The Evolution of Transport Network Survivability", *IEEE Commun. Mag*., vol. 37, no. 8, Aug 1999, pp. 44-51

[15] *Sosnosky, J., Lin, Z.*, " Planning for Broadband Multilayer Survivability," T1X1.5, May 1999.

[16] *Bonenfant, P., Ballintine, J., Newsome, G.*, "Optical Transport Networking with 'Digital Wrappers", *Optical Internetworking Forum OIF 99.011*, Jan. 1999.

[17*] Haskin, D., Krishnan, R.*,"A Method for Setting an Alternative Label Switched Paths to Handle Fast Reroute", *IEFT Draft draft-haskin-mpls-fast-reroute-01.txt*, June 1999.

[18] *Doshi, B., et al.*, "Optical Network Design and Restoration", *Bell Labs Technical Journal*, Vol. 4, No.1, January-March 1999, pp. 58-84.

[19] *Shew, S.*, "Fast Restoration of MPLS Label Switched Paths," Internet draft, work in progress, June 1999.

[20] *Medard, M.*, et al, "Security issues in all-optical networks," *IEEE Network*, pp. 42-48, May/June 1997.